Engineering Principles – An Introduction

Key Engineering Principles

&

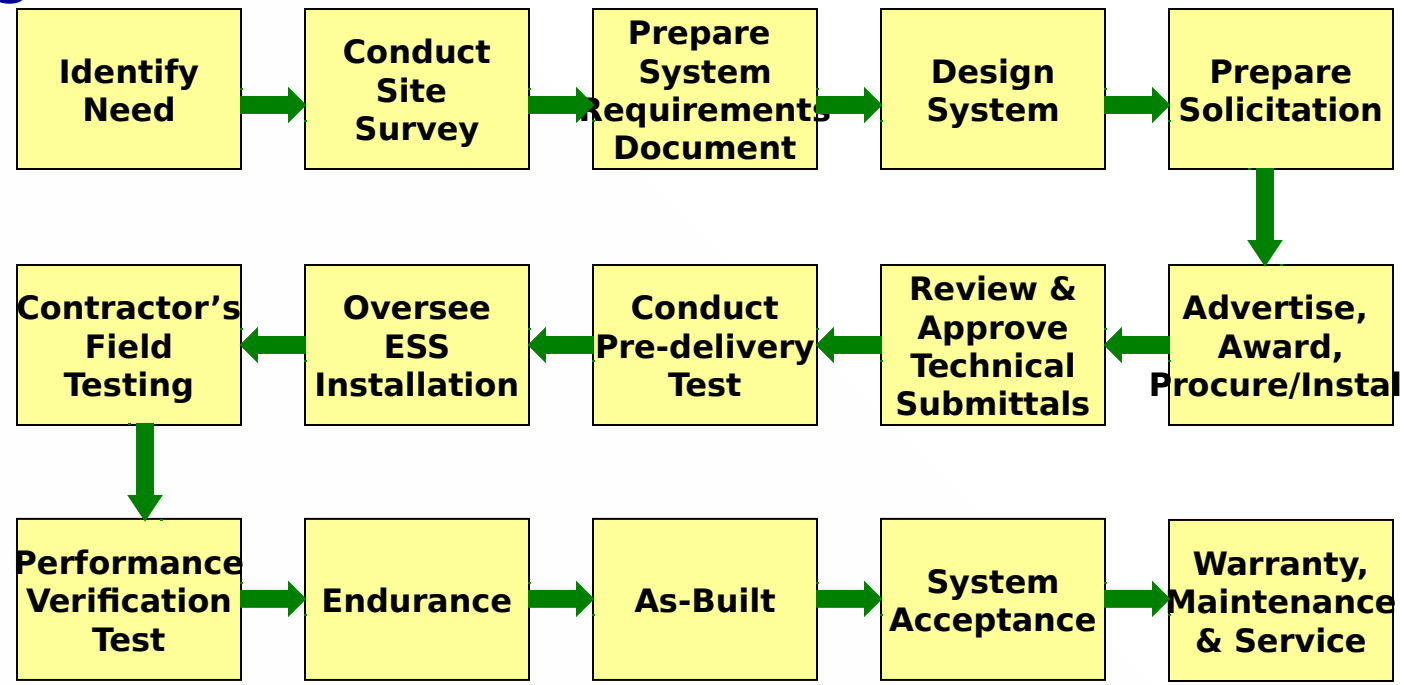
Security Philosophy

of

ESC Business

ESS Implementation

ESS implementation, whether a brand new system or an upgrade of an existing system, will generally progress as follows…



Test! Test! Test!

Don't forget training!

Measure twice, cut once…an engineering solution!

Security Concepts and Philosophies

- Asset
- Threat
- Risk
- Risk Management
- Protection in Depth
- Balanced Protection
- Detect, Assess, Delay, Respond

Asset

- What are we protecting and what are we protecting against?
- Asset – an item with some value (qualitative or quantitative) worth protecting.

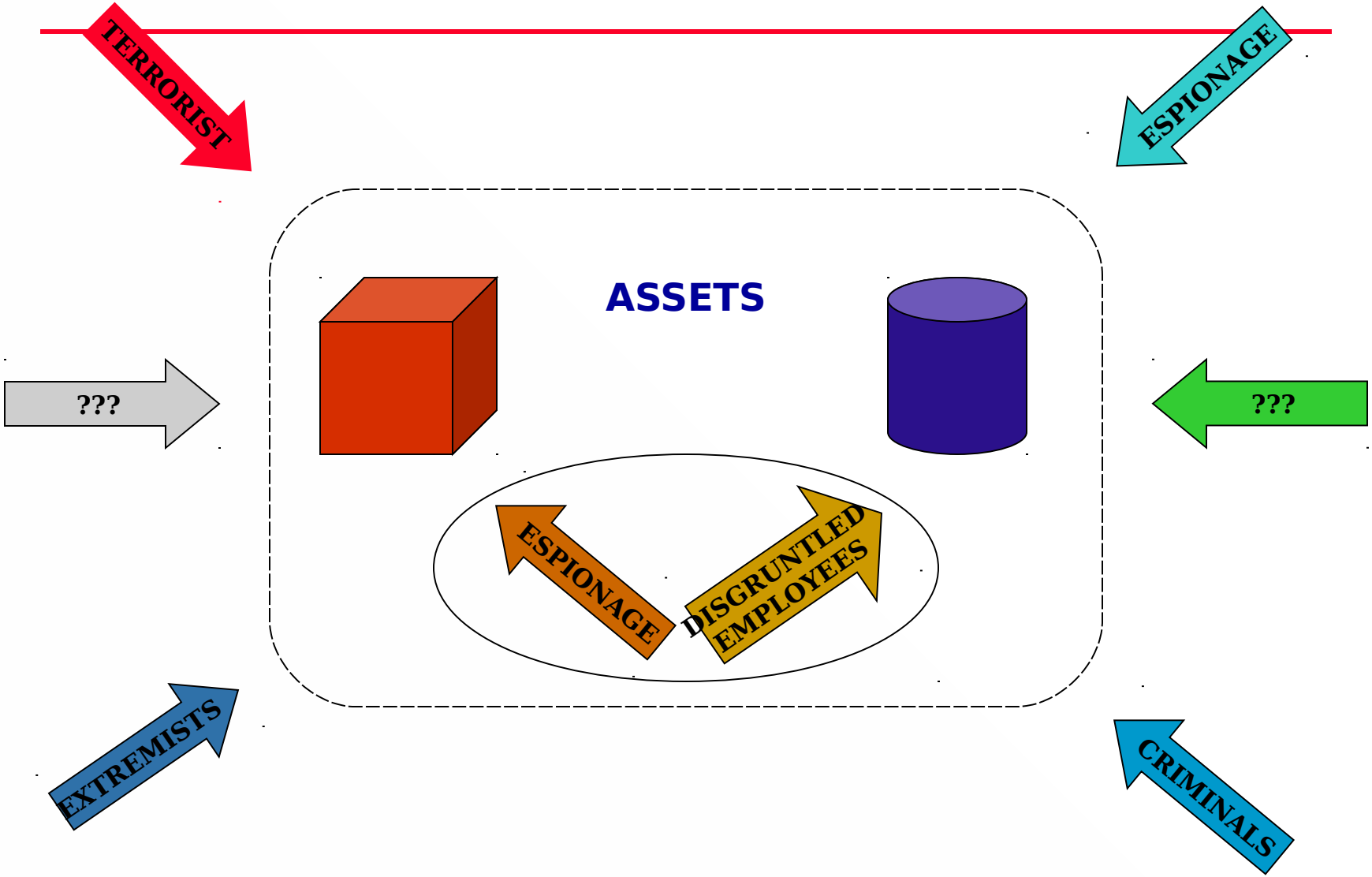
What is Threat?

- Can be Natural or Man-made
- Possible Aggressor Acts That May Result In:
  - Sabotage or Theft of Information
  - Inflicting Injury or Death on Personnel
  - Damage, Loss or Destruction of Facilities and Equipment
  - Disruption or Failure of Missions
  - Denial of Services
  - Creating Adverse Publicity

Installation Threat Statement

- **Usually Classified**
- **Designer Must Consider the Threat**
- **May Require Additional Measures for Comprehensive Protection**

Potential Threats



What is Risk?

- Risk is a function of:
  - Threat
  - Consequence of loss of the protected asset
  - Vulnerability
- Risk is difficult to measure.
- Risk can be shifted or mitigated but rarely eliminated.
- Risk is more often expressed in a qualitative manner, such as High, Medium and Low rather in quantitative terms.

What is Risk? (cont'd)

- **Risk measurement involves identifying the likelihood that the risk will create an impact on, and have consequences with respect to the well-being of persons or continued operations.**
- ***Threat events*** **can be described in terms of damage which will occur; or probability of the event's occurrence, while…**
- ***Risk*** **can be described in terms of its potential occurrence and its capacity for potential loss.**

Risk Management

- **Risk management principles include assessment of assets, threats and vulnerabilities, analyzing risks, then mitigating the risks by employing effective countermeasures.**
- **Various codes, standards and regulations are available to guide the management of risk.**
- **Codes, Standards & Regulations**
  - **USACE ESS Standards**
  - **Agency Regulations**
  - **Industry Standards**
  - **Local Codes**

Protection - In - Depth

Protection in Depth:

- **Adversary is Required to Defeat a Number of Protective Devices In Sequence (i.e. sensors, barriers)**
- **Minimizes Effect of Component Failure**
- **Includes Procedures and People in Addition to Hardware**

Balanced Protection

Balanced Protection:

No matter how an adversary attempts to accomplish their goal, effective elements of the physical security system will be encountered (i.e. walls, doors, roof hatch, HVAC vents, and windows must have comparable penetration resistance).

Detect, Assess, Delay, Respond

- **Detect**
  - **Probability of Detection**
  - **Time for Alarm Communication**
- **Assess**
  - **Time for Assessment**
- **Delay**
  - **Time to Defeat Obstacles**
- **Respond**
  - **Probability of Accurate Communication to Responders**
  - **Time to Communicate with Response Force**
  - **Probability of Deployment to Adversary Location**
  - **Time to Deploy**
  - **Response Force Effectiveness**

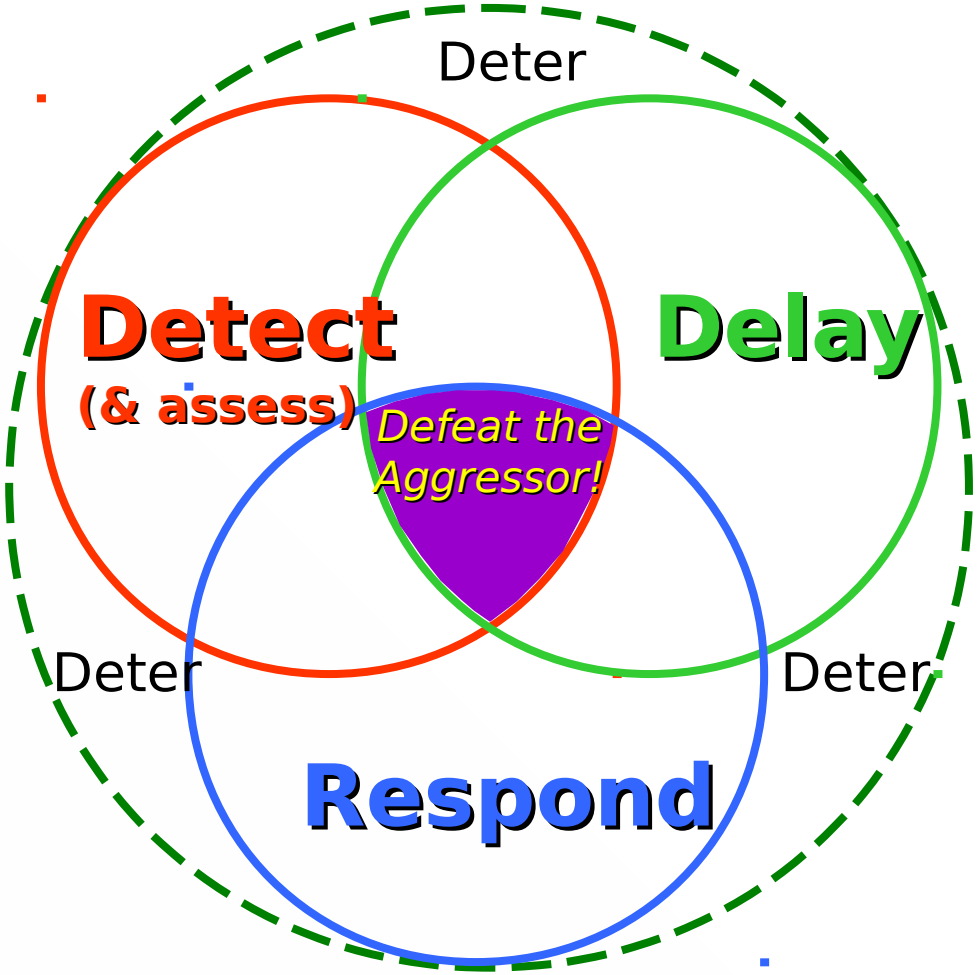
Detect, Assess, Delay, Respond (cont'd)

- **Detect before Delay – Detection is most effective at the perimeter.**
- **Delay is more effective at the target.**
- **Detection is not complete without assessment.**
- **The total time for detection, assessment, delay, and response must be less than the adversary's task time to the asset.**

Physical Security Model

ESS is only one component of physical security…

- ESS enhances the probability of detecting an aggressor before he compromises a protected asset.
- Delay and response elements are required to defeat the aggressor after he is detected.

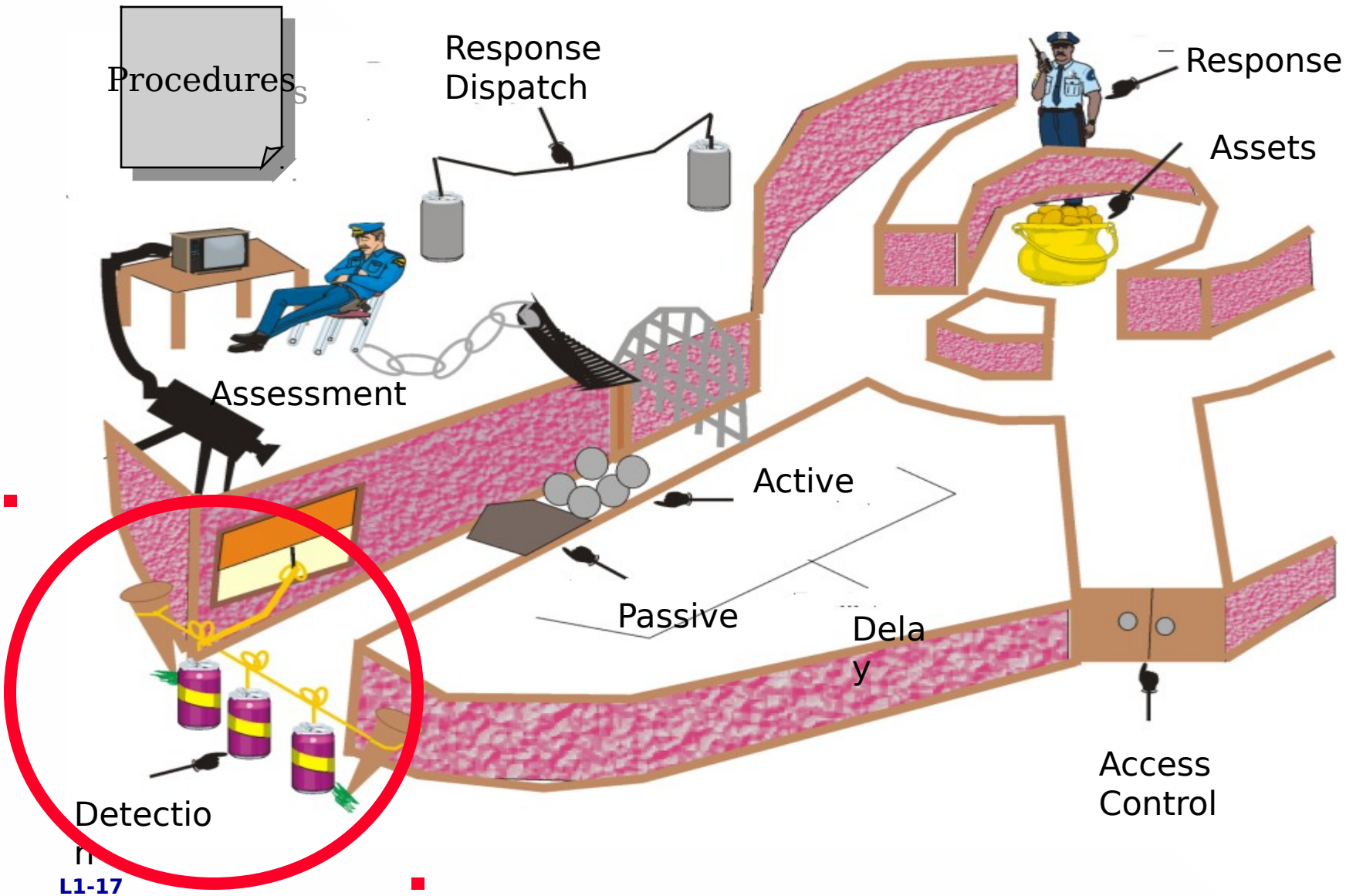


Physical security is that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. (Excerpt from Army Regulation 190-16)

Detect

- **Sensing a Specified Target Moving Through a Line of Demarcation**
  - **Always Requires Motion**
  - **Consists of Sensors Suitable for Expected Target**
  - **Limited to an Area Free of Likely Nuisance Alarm Sources**
  - **Continuous in a Ring or Area Surrounding Assets**

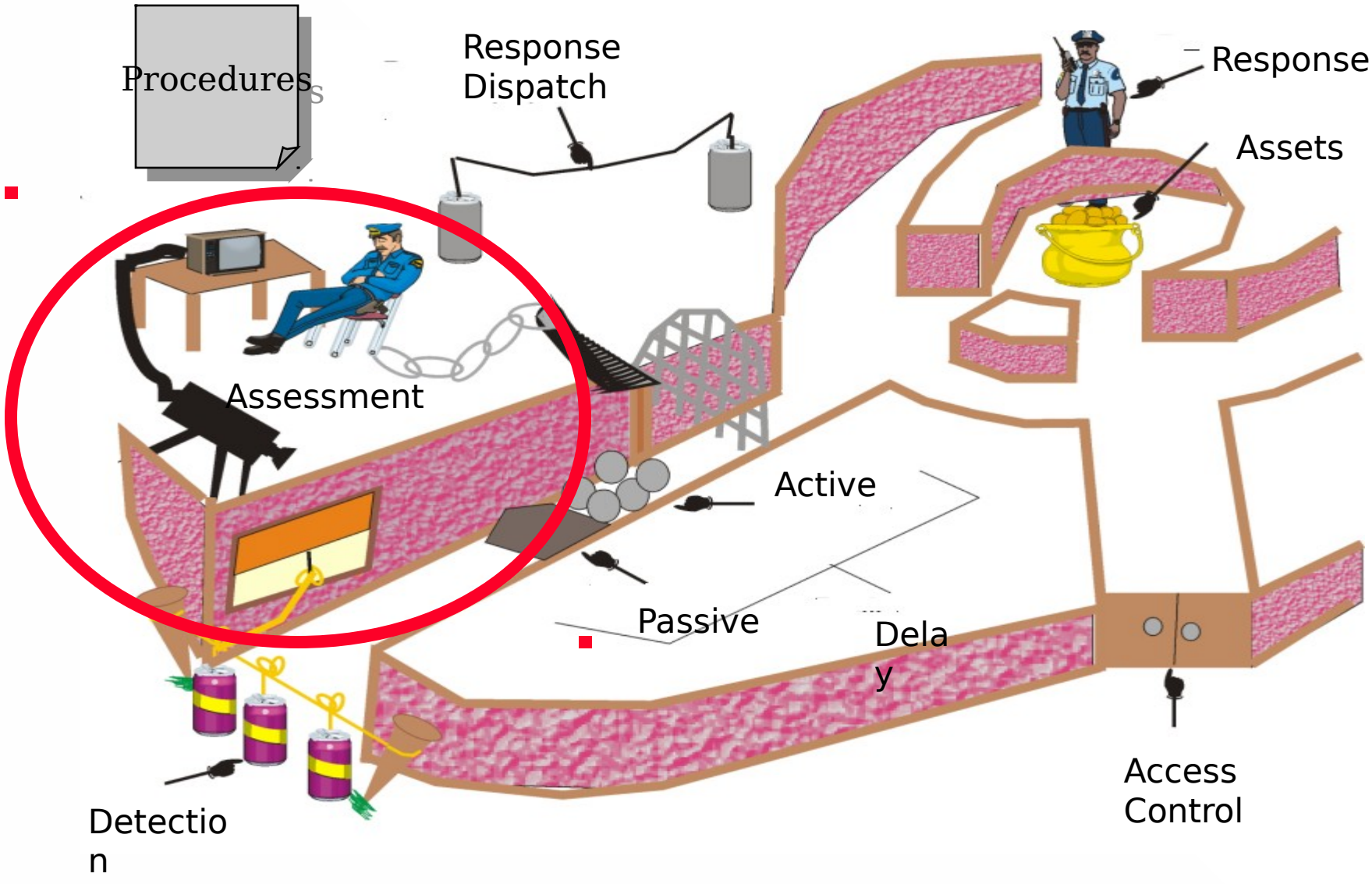
Functional Elements of an Effective Security System



Assess

- Evaluation of a Detected Target to Determine Level of Threat Against Assets
  - Validates a Detection As a Threat or Nuisance
  - Offers Additional Information About Target
    - Direction of Movement
    - Speed of Movement
    - Numbers of Targets
    - Tools or Armament of Targets
  - Coordinated With Detection
  - Information May Assist Response Forces
- Assessment is Time Sensitive
  - Guard Direct Assessment
  - Guard CCTV Remote Assessment

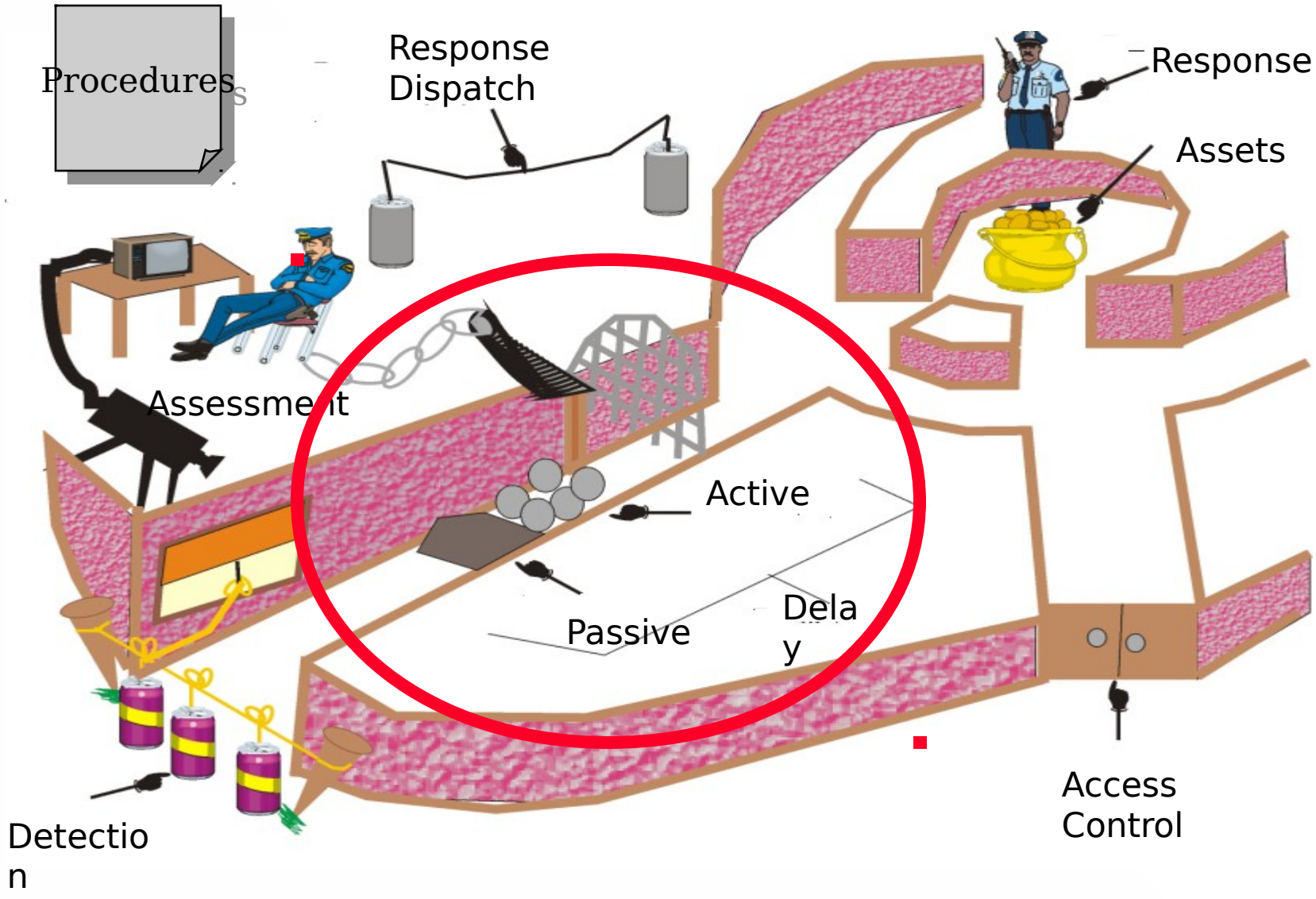
Functional Elements of an Effective Security System



Delay

- **Features That Slow Intruders Until Response Forces Can Intercept**
  - **Consists of Some Form of Barrier**
    - **Man-Made or Natural**
    - **Active or Passive**
  - **Barriers Are Often Tailored for Selected Threat Characteristics**

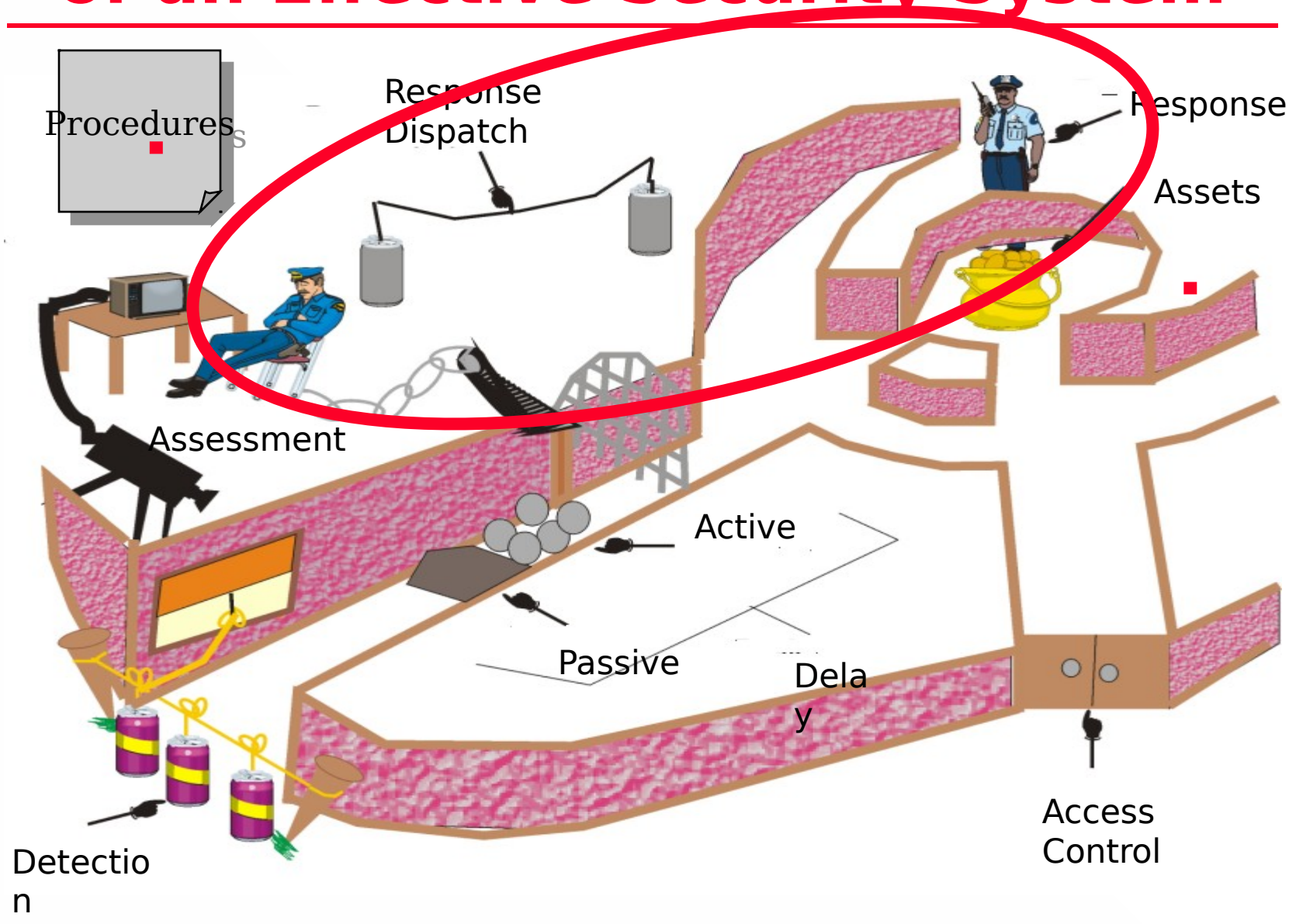
Functional Elements of an Effective Security System



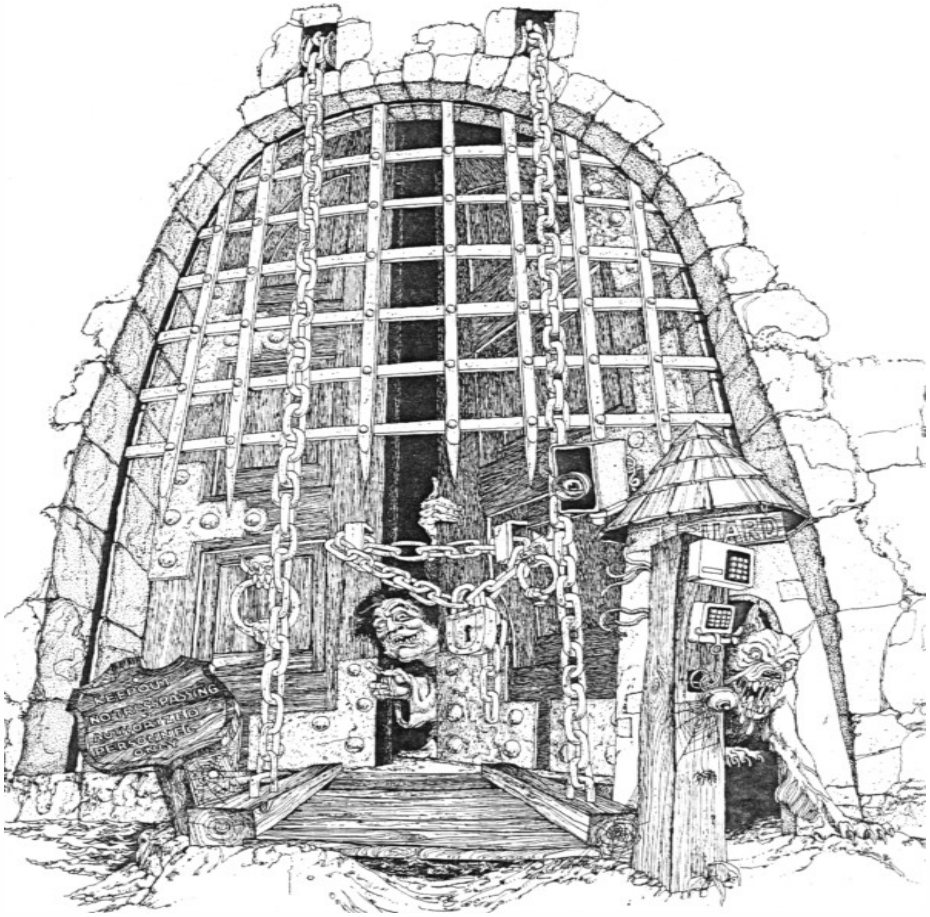
Respond

- **Action Taken to Prevent Intruders From Accomplishing Their Objectives Against the Assets**
  - **Consists of Response Force, Weapons, Vehicles, Communications, and Tactics**
  - **Deployment Time Influences System Response Time and Delay Time Requirements**
  - **Must be Structured to be Effective for an Entire Range of Intrusions**
- **Security Strategy**
  - **Denial**
  - **Containment**
  - **Forensic**

Functional Elements of an Effective Security System



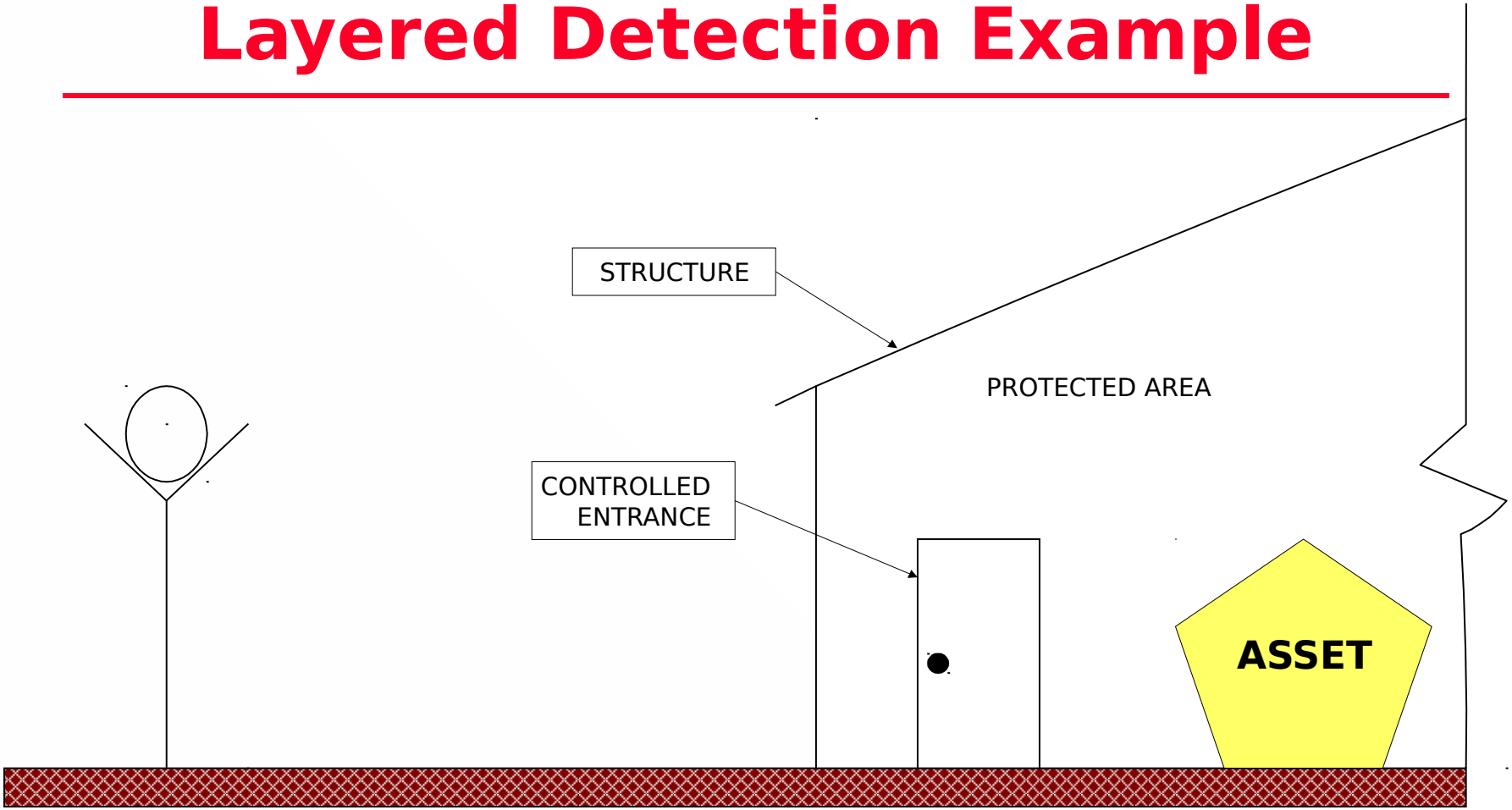
Entry Control



Layered Detection

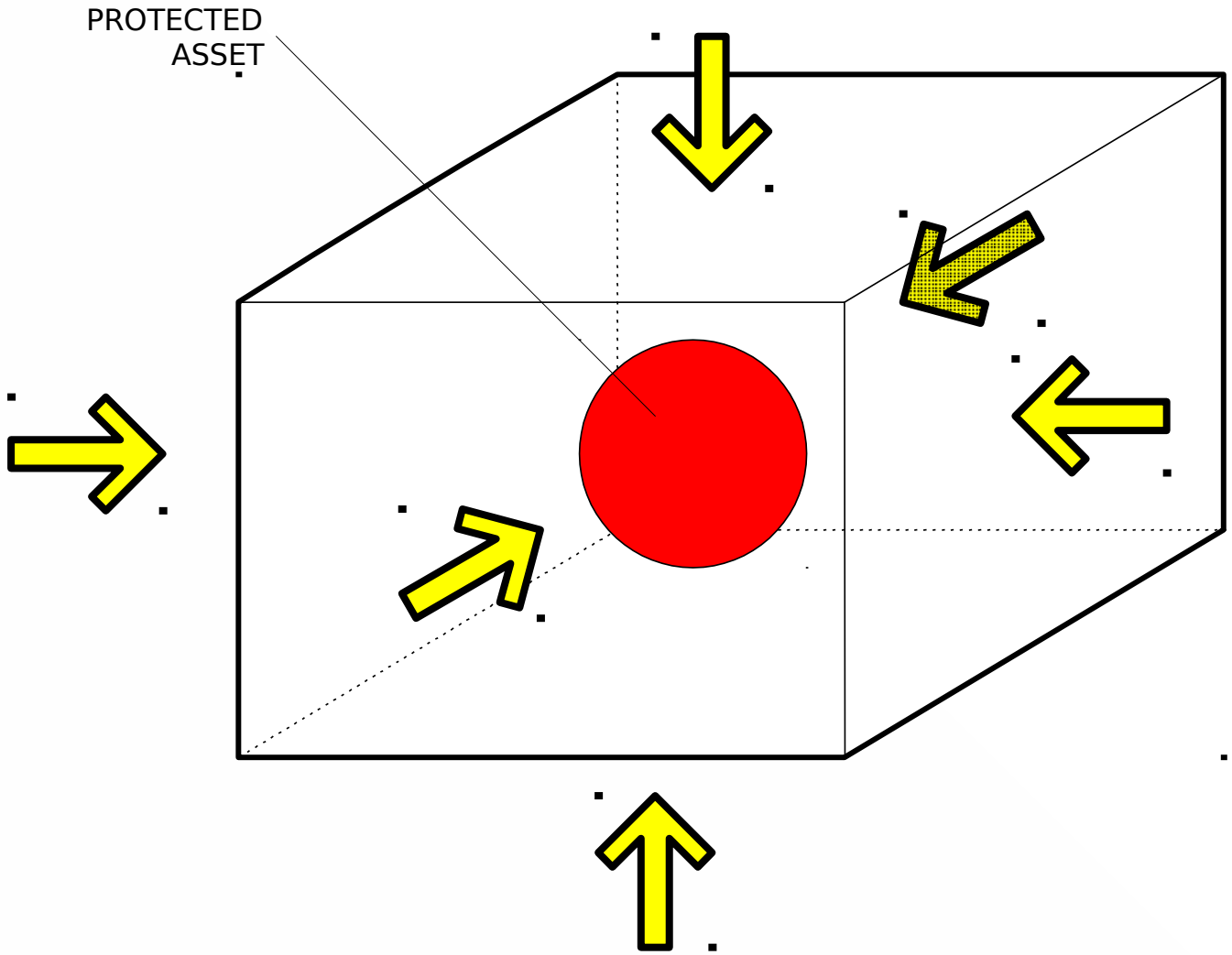
- Generally Categorized as Interior and Exterior Sensor
- Incorporates Concentric Rings of Protection
- Starts as Far From the Facilities/Assets As Conditions Will Allow
- Provides Operationally Effective and Suitable Countermeasures
- Provides Cost Efficiencies

Layered Detection Example

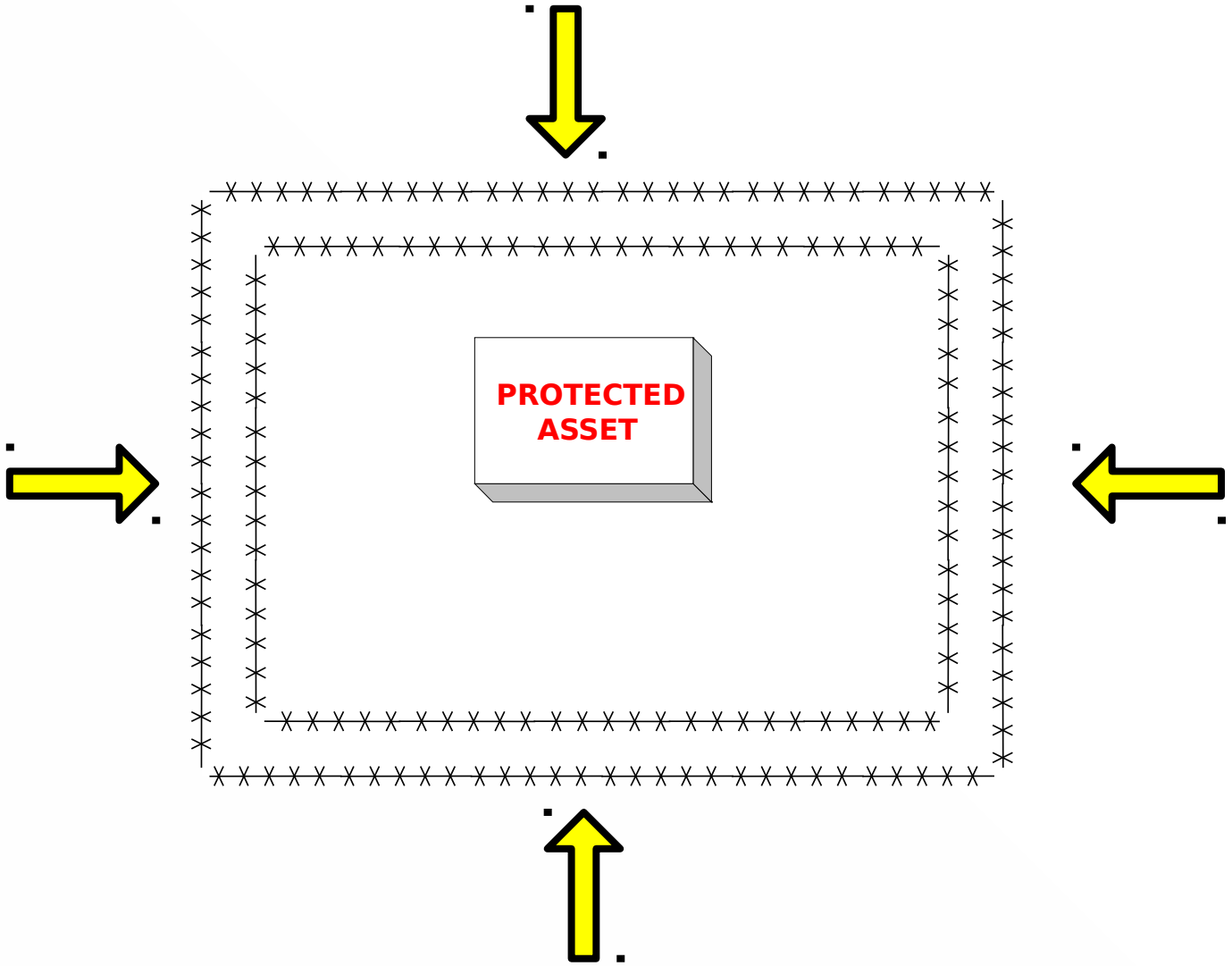


PERIMETER DETECTION	EXTERIOR DETECTION	BOUNDARY PENETRATION DETECTION	VOLUMETRIC DETECTION	POINT DETECTION

Interior IDS

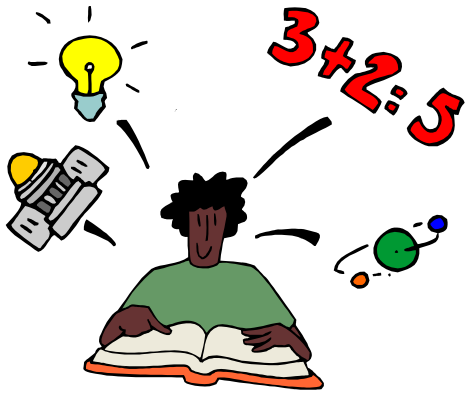


Exterior IDS



Sensor Phenomenology

- **No Perfect Sensor**
- **Different sensor types have different:**
  - **Strengths**
  - **Weaknesses**
  - **Vulnerabilities**



- **Site Preparation Requirements**
- **Life Cycle Cost Comparisons**

Probability of Detection (PD)

- Measure of a Sensor's Performance
- Dimensionless Number Between 0 and 1
- Confidence Level Determines Number of Samples Required
- Method of Testing Performance Must be Carefully Defined
- Beware! - Probability of Detection is conditional
  - Target characteristics
  - Sensitivity settings
  - Sensor hardware
  - Weather conditions
  - Installation workmanship
  - Maintained condition

Alarm Definitions

- **Intrusion Alarm: Annunciation of an Alarm Resulting from the Detection of a Specified Target that Represents an Attempt to Intrude into the Protected Area**
- **Nuisance Alarm: Annunciation of an Alarm Resulting from the Detection of a Target that Is Not an Attempt to Intrude into the Protected Area**
- **Environmental Alarm: Annunciation of an Alarm Resulting from Environmental Conditions that Exceed Specified Limits**
- **False Alarm: Annunciation of an Alarm Resulting from No Apparent Cause**

Alarm Type Responsibilities

- **Installation Contractor Typically Responsible for:**
  - **Intrusion Alarm Performance**
  - **False Alarm Performance**
- **Installation Contractor Typically NOT Responsible for:**
  - **Nuisance Alarm Performance**
  - **Environmental Alarm Performance**
- **Nuisance and Environmental Alarms may be the Result of Poor Design**

Nuisance Alarm Rate (NAR)
False Alarm Rate (FAR)

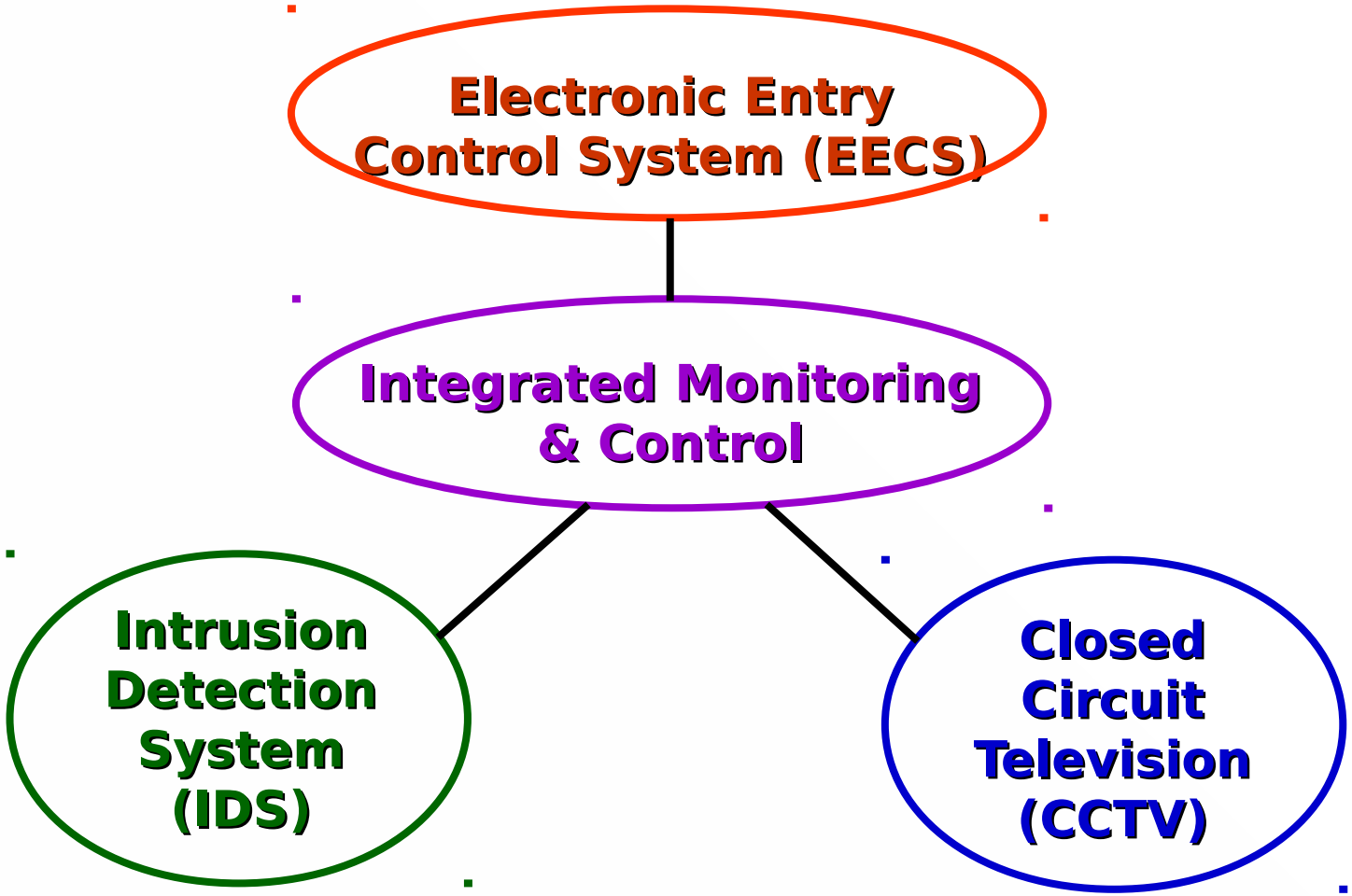
- Number of Nuisance or False Alarms Per Unit of Time
- Measured at Specified Probability of Detection
- Weather and Terrain Can Adversely Impact NAR
- High NAR/FAR Reduces Operator Confidence in System

Vulnerability to Defeat

- As Important as PD and NAR/FAR
- Defeat Resistance Includes
  - Choosing Correct Sensor for the Environment
  - Tamper Protection
  - Signal Line Supervision
  - Proper Installation Techniques
  - Physical Construction
  - Overlapping Sensor Detection
  - Multiple Sensor Phenomenologies

Technology Summary

An electronic security system (ESS) consists of three integrated subsystems...


Electronic Entry Control System (EECS)
Integrated Monitoring & Control
Intrusion Detection System (IDS)
Closed Circuit Television (CCTV)

Functional Elements of an Effective Security System